北京大学
PEKING UNIVERSITY

物理不可克隆函数概述及应用

组会分享

分享人：时　林

时间：2021.09.28

目录

CONTENTS

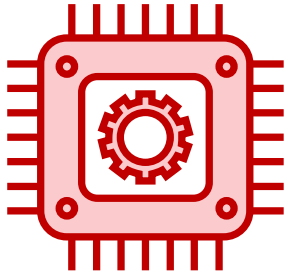
1 PUF相关概述

Overview of PUF

什么是物理不可克隆函数

世上没有两片完全相同的树叶。

——戈特弗里德·威廉·莱布尼茨



那么世界上是否存在两个完全相同的芯片？

不可能

物理不可克隆函数

没有两个物体是完全一样的，即使采用相同的工艺来制造它们。虽然我们通常不希望制造过程中产生差异，但是为了安全目的，可以利用和这些差异的相关作用来唯一地识别物理对象。为了便于实现这种作用，可以在集成电路（IC）上实现所谓的**物理不可克隆函数（Physical Unclonable Function ,PUF）**。

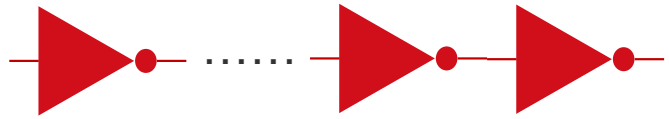
不可克隆函数

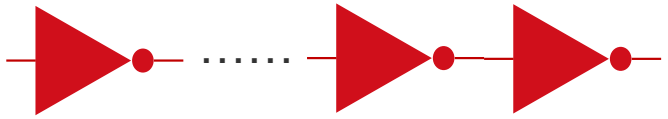
随机性物理差异具有**难以克隆或伪造的天然特征**，因为完全控制物理介质中的微米和纳米级制造差异是非常困难的， 并且即使可能实现，也是非常昂贵的。

$$C_i \longrightarrow R_{Ci}$$

PUF的类型

The **time delay** $T_1 == T_2$?





$$S_{Ci} = T_i$$

PUF主要实现

	PUF类型	PUF具体实现	
PUF	非电子PUF	光学PUF	
		纸PUF	
		CD PUF	
	模拟电路PUF	基于涂层的PUF	
		基于阈值电压的PUF	
		基于电阻的PUF	
	数字电路PUF	基于存储的PUF	基于仲裁器的PUF
			基于环形振荡器的PUF
			毛刺PUF
		基于延迟的PUF	触发器的PUF
			SRAM PUF
			蝴蝶PUF
			锁存PUF

PUF的属性

PUF概念

- **物理激励-响应函数**：PUF的输入一般称为**激励**；输出一般称为**响应**。
- **片间汉明距离**：对**两个不同** PUF 实体输入一个特定的激励后，其产生的两个响应之间的距离或者差异。
- **片内汉明距离**：对一个**单一**的 PUF 重复两次输入一个特定的激励后，其产生的响应之间的差异。

从PUF实现方法的归类总结，可以看出PUF**并不是一个单纯的的数学概念**，而是嵌入了物理实体，包含诸多属性有输入输出功能的**函数**。为了更好地理解PUF的基本特性，这里给出PUF的常见的**基本属性**[1]。

[1] Zhang J L, Qu G, Lv Y Q, et al. A survey on silicon PUFs and recent advances in ring oscillator PUFs[J]. Journal of computer science and technology, 2014, 29(4): 664-678.

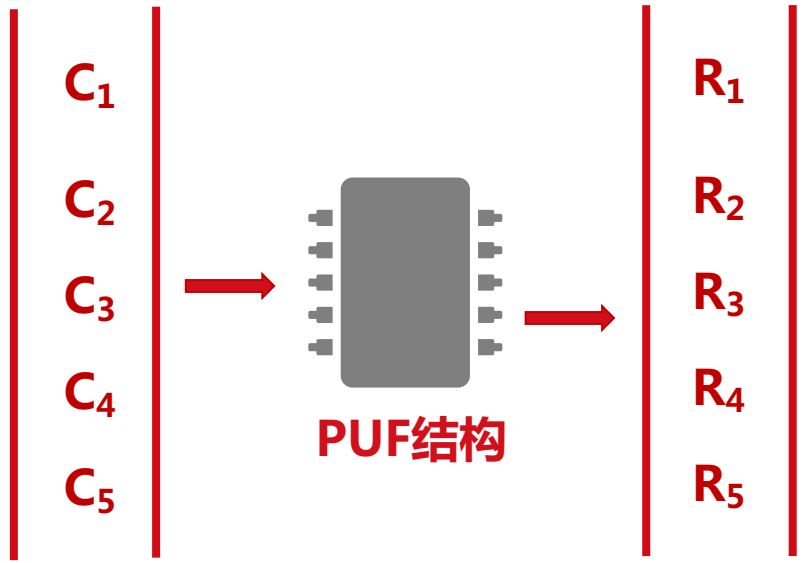
Challenge-Response Pairs

挑战应答方式”：**Challenge-Response**，是零知识证明的方式。

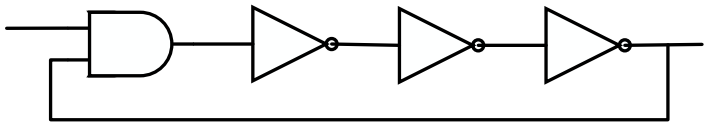
Challenge Response Pair：特定PUF产生的**激励响应对（CRP）**，并且满足唯一标识。

基于挑战/应答的身份认证

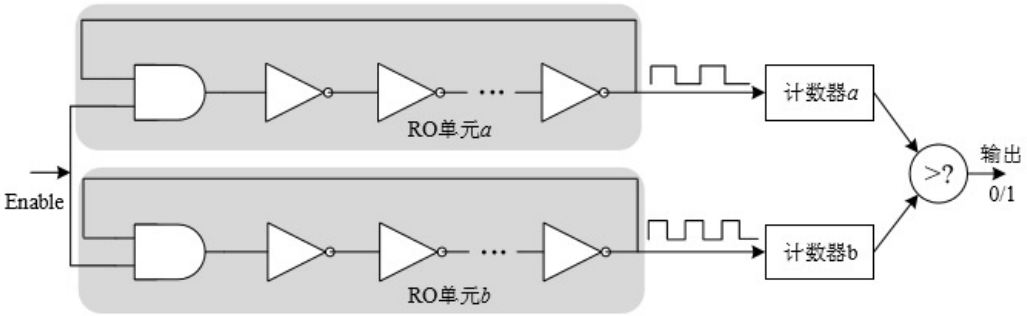
PUF产生的Challenge Response Pair



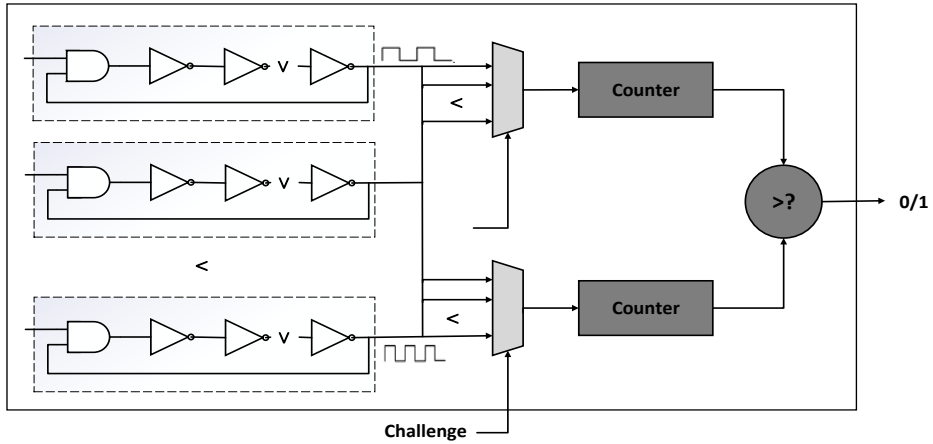
RO PUF



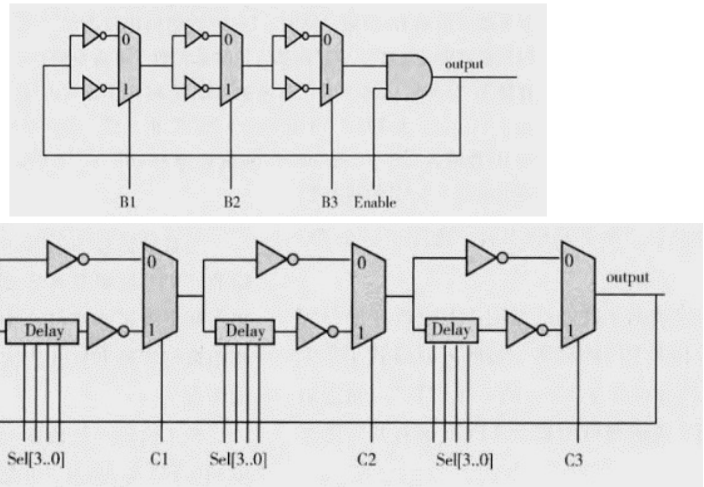
基本环形振荡器（Ring-Oscillator,RO）结构



RO PUF基本工作原理



传统RO PUF



可配置的RO PUF

2 当前PUF的应用

Application of PUF

传统物联网安全机制的限制

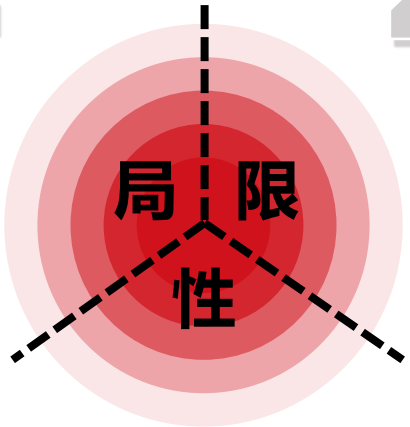
传统的安全机制

- 在EEPROM中存储密钥；
- 在电池支持的SRAM中存储密钥；
- 结合密码算法实现信息加密和认证；

传统技术局限性

1 计算资源受限

2 存储资源受限

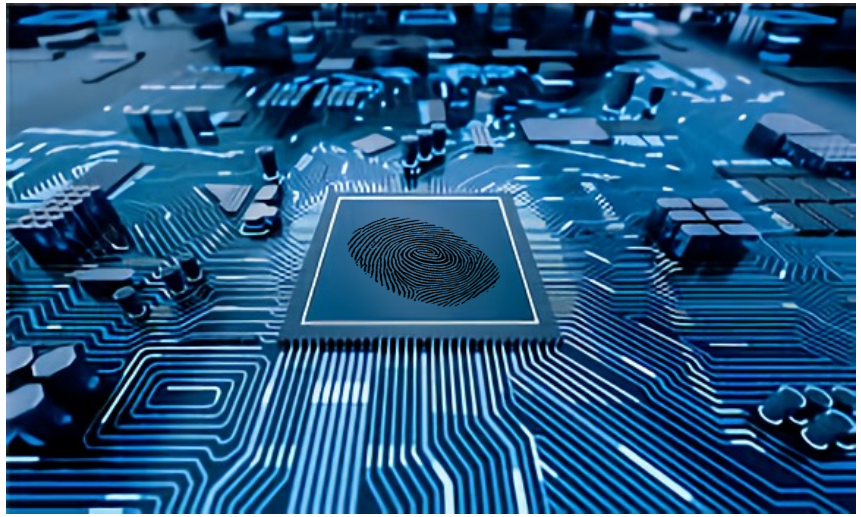


……

PUF技术的相关应用

芯片制作差异产生的天然特征

——芯片“指纹”



$$C_i \longrightarrow \mathrm{R}_{Ci}$$

当前PUF的发展

当前，物理不可克隆函数在工业界已有了相关的应用，但仍有着限制和挑战。

PUF的应用

- 身份认证
- 密钥生成器/种子
- 安全协议

当前存在的限制

PUF为每个设备生成芯片唯一密钥，并且无法在另一个设备中克隆。

面临的挑战

PUF具有不可克隆性和唯一性的特点，同样的PUF在不同的设备上指纹是不同的，想要在不同的设备利用PUF生成相同的密钥进行共享，这与PUF的唯一性原则相悖。

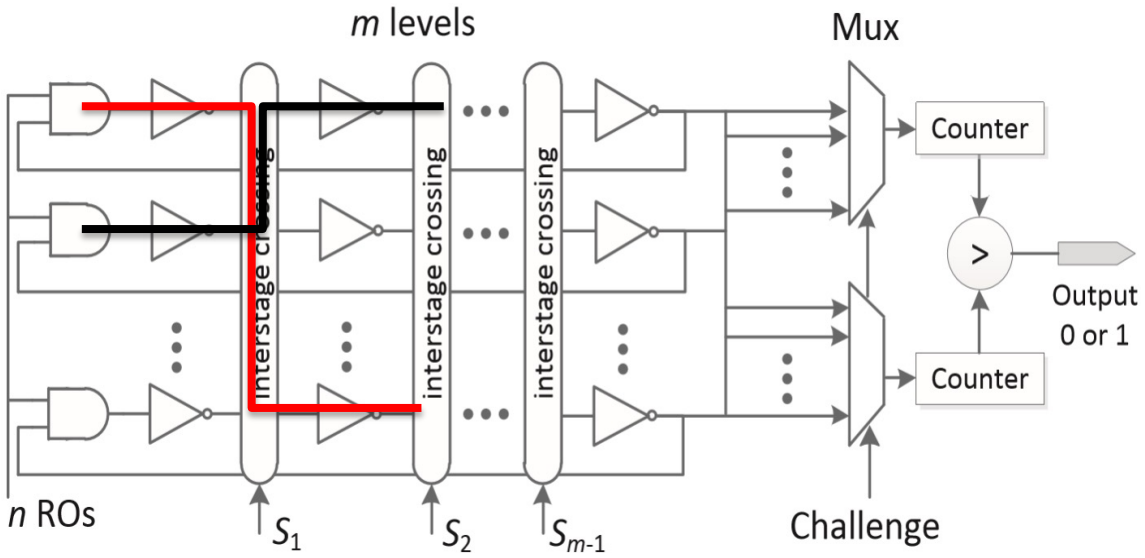
3 PUF密钥共享

Key Sharing Base on PUF

级间交叉的PUF

CRO PUF

传统的RO PUF中反相器固定排列，通过Challenge对得到的Response**情况有限**，不能很好的利用所有的反相器。所以为了提高PUF结构的灵活性，CRO PUF引入了**配置位S**来对每两列反相器之间的连接进行配置，极大的**增加了反相器组合的可能性**。



CRO PUF设计图

共享密钥生成原理

延迟矩阵模型

带有**k**个反相器的**n**行CRO PUF的**延迟模型**如下所示：

$$Delay_{RO}=\begin{matrix} d_{11} & d_{12} & \cdots & d_{1j} & \cdots & d_{1k} \\ d_{21} & d_{22} & \cdots & d_{2j} & \cdots & d_{2k} \\ \vdots & \vdots & & \vdots & & \vdots \\ d_{i1} & d_{i2} & \cdots & d_{ij} & \cdots & d_{ik} \\ \vdots & \vdots & & \vdots & & \vdots \\ d_{n1} & d_{n2} & \cdots & d_{nj} & \cdots & d_{nk} \end{matrix}$$

每一行的**延迟向量** $D_{RO}=\{D_1,D_2,\dots,D_i,\dots,D_n\}$，其中 $D_i=\sum_{j=1}^{k}d_{ij}$。**选择信号** $S=\{S_1,S_2,\dots,S_j,\dots,S_{k-1}\}$，$S_j$控制着第j和第j+1列反相器之间的**连接路径**。

实例：

以**两个CRO PUF**为例，每个CRO PUF 都包含四个4层反相器，相应的延迟模型分别由**矩阵A**和**矩阵B**表示。

$$A=\begin{matrix} 3 & 6 & 8 & 5 \\ 9 & 7 & 4 & 5 \\ 5 & 4 & 6 & 5 \\ 2 & 5 & 6 & 3 \end{matrix} \quad B=\begin{matrix} 2 & 4 & 6 & 5 \\ 5 & 1 & 3 & 2 \\ 8 & 6 & 5 & 7 \\ 3 & 6 & 4 & 5 \end{matrix}$$

考虑下面这**两个challenge**：

$C_A=\{\{1,2\},\{2,3\},\{3,4\}\}$

$C_B=\{\{1,3\},\{3,4\},\{4,2\}\}$

在这种情况下，**两个CRO PUF**的Response都是**{0,1,1}**。

同样的，假设challenge是：

$C_A=\{\{4,2\},\{2,3\},\{3,1\}\}$

$C_B=\{\{1,2\},\{2,4\},\{4,3\}\}$

保持A中的**选择信号S不变**，调整B中的**S2和S4**，路径延迟模型变成：

A和B的延迟向量变成：

$$A=\begin{matrix} 3 & 6 & 8 & 5 \\ 9 & 7 & 4 & 5 \\ 5 & 4 & 6 & 5 \\ 2 & 5 & 6 & 3 \end{matrix} \quad B=\begin{matrix} 2 & 4 & 6 & 5 \\ 5 & 6 & 3 & 7 \\ 8 & 1 & 5 & 5 \\ 3 & 6 & 4 & 2 \end{matrix}$$

$D_A=\{22,25,20,16\}$

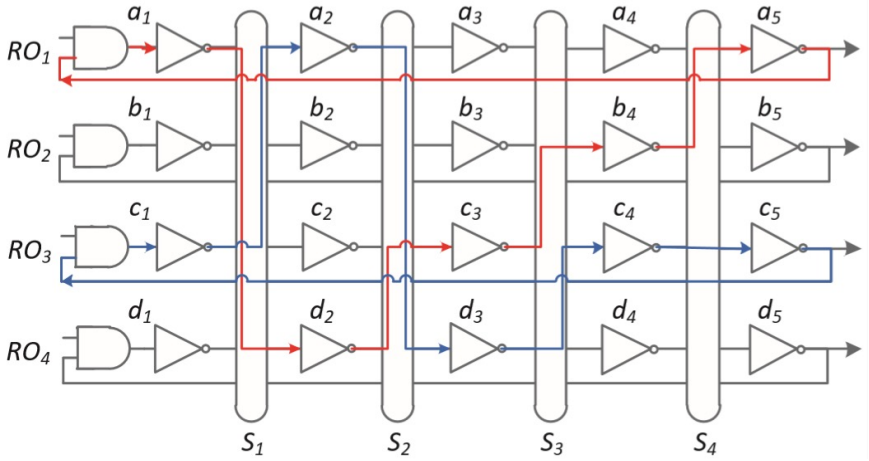
$D_B=\{17,21,19,15\}$

这种情况下，**两个CRO PUF**的Response都是**{0,1,0}**。

共享密钥生成原理

延迟矩阵建模

采用**机器学习**的方法对**延迟矩阵**进行建模。

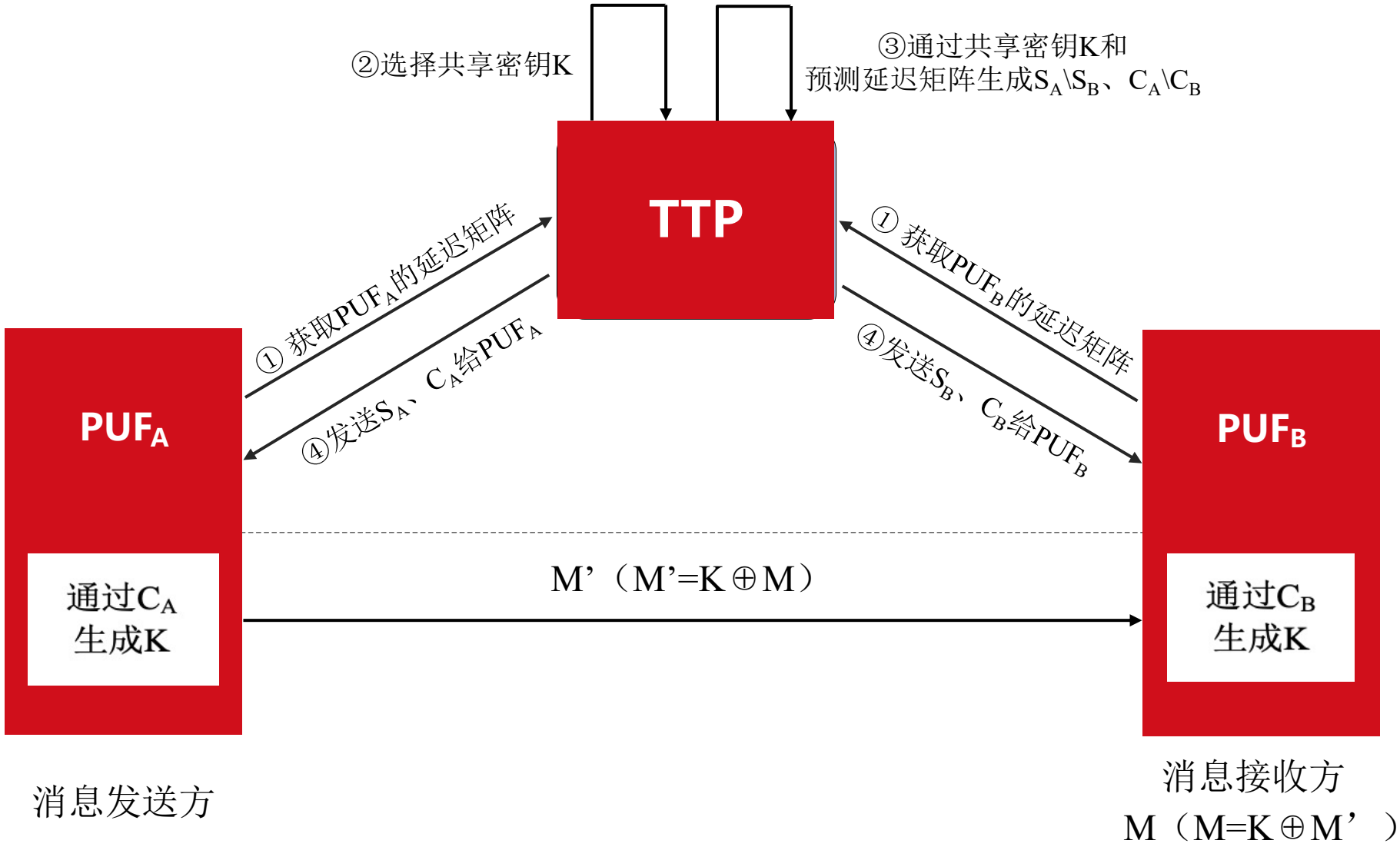


$$C=\begin{matrix}1&0&0&0&1\\0&0&0&1&0\\0&0&1&0&0\\0&1&0&0&0\end{matrix}\quad W=\begin{matrix}a_1&a_2&a_3&a_4&a_5\\b_1&b_2&b_3&b_4&b_5\\c_1&c_2&c_3&c_4&c_5\\d_1&d_2&d_3&d_4&d_5\end{matrix}$$

计数器中的数字计数可以由公式给定： $Counts=\frac{1}{C\cdot W}$

在已知延迟矩阵的情况下，通过设置不同的配置位 S_i 和激励,从而使得多方生成相同的输出。

密钥共享协议


②选择共享密钥K
③通过共享密钥K和预测延迟矩阵生成S_A\$S_B$、$C_A$\$C_B$
TTP
① 获取PUF_A的延迟矩阵
④发送S_A、C_A给PUF_A
① 获取PUF_B的延迟矩阵
④发送S_B、C_B给PUF_B
PUF_A
PUF_B
通过C_A生成K
M’（M’=K⊕M）
通过C_B生成K
消息发送方
消息接收方
M（M=K⊕M’）

安全性分析

建模攻击

没有可访问的接口能够读取芯片内部生成的响应（response），因而无法获取CRPs，无法进行机器学习建模。

密钥共享协议的安全分析

——Scyther协议分析工具

Scyther给出的两种可能的攻击方法均假设了攻击者知道原始的PUF模型或预先训练好的PUF模型。

测信道攻击

动态的改变RO反相器的配置数据，从而生成持续更新的密钥，使得每个RO都没有固定的物理位置。

4 总结与展望

Summary and Prospect

PUF的研究前景

PUF领域的相关研究已经有了很大的进展。无论是在如**RFID、智能卡**等资源有限设备中，还是在相对成熟的**密码学应用**中；无论是在硬件安全领域的**认证应用**中，还是在软件的密钥生成等**算法协议**中，PUF都凭借其具有不可克隆性、防篡改、轻量级等良好的属性，发挥着**不可替代**的作用。

形式化定义

在现实安全应用中，PUF的形式化定义是PUF的设计、开发与应用正确性的基础与保证。然而目前提出的PUF实现方法的一些形式化定义都或多或少存在一些问题[1]，要么被限制太多，即不包括某些类型的PUF，要么太虚拟化，甚至假设某些PUF的属性。从这个意义上讲，如何给出PUF及其属性的严格的形式化定义，仍需要进一步深入的研究。

系统设计方法

在过去的几年间，虽然人们提出了大量的PUF实现方法，但是通过总结比较发现，这些实现方法的设计都是在孤立的条件下提出的。换句话说，PUF实现方法的设计都具有临时性。那么是否可以提出PUF实现方法的系统设计方法，以便人们根据具体的情况来设计实现PUF。

轻量级界限

在RFID传感器网络节点等资源有限的设备中,基于轻量级属性的PUF可以实现大量的应用。但是，前人的工作只是在广泛的意义上提出了PUF的轻量级属性，并没有给出PUF轻量级属性的具体界限。虽然有大量的PUF的实现方法和应用，但在这方面却很少有研究。所以使用什么样的理论来考虑、解决这个问题,将是一个全新的研究方向。

[1] Rührmair U, Sölter J, Sehnke F. On the foundations of physical unclonable functions[J]. IACR Cryptol. ePrint Arch.

论文总结

ICC.2021:Communication Security in VANETs based on the Physical Unclonable Function.

ISSCC.2021:Unified In-Memory Dynamic TRNG and Multi-Bit Static PUF Entropy Generation for Ubiquitous Hardware Security.

IDC.2021:On the Security of Strong Memristor-based Physically Unclonable Functions.

DATE.2020:Reliable and Lightweight PUF-based Key Generation using Various Index Voting Architecture.

CASES.2020:The Shift PUF: Technique for Squaring the Machine Learning Complexity of Arbiter-based PUFs: Work-in-Progress.

ICCE.2020:Embedded Systems Authentication and Encryption Using Strong PUF Modeling.

DSN.2019:DeviceVeil: Robust Authentication for Individual USB Devices Using Physical Unclonable Functions

THANKS !

北京大学

PEKING UNIVERSITY